PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A1

(11) International Publication Number: **WO 98/58305**

(43) International Publication Date: 23 December 1998 (23.12.98)

(21) International Application Number: PCT/GB98/01705

(22) International Filing Date: 11 June 1998 (11.06.98)

(30) Priority Data:
9712505.8 16 June 1997 (16.06.97) US

(71) Applicant *(for all designated States except US)*: MEMORY CORPORATION PLC [GB/GB]; The Computer House, Dalkeith Place, Dalkeith, Edinburgh EH22 2NA (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DEAS, Alexander, Roger [GB/GB]; 8 Eskview Grove, Dalkeith, Edinburgh EH22 1JW (GB). McCOLL, Cameron [GB/GB]; "Hillwoodlea", Roslin, Edinburgh EH25 9RD (GB).

(74) Agents: McCALLUM, William, Potter et al.; Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE (GB).

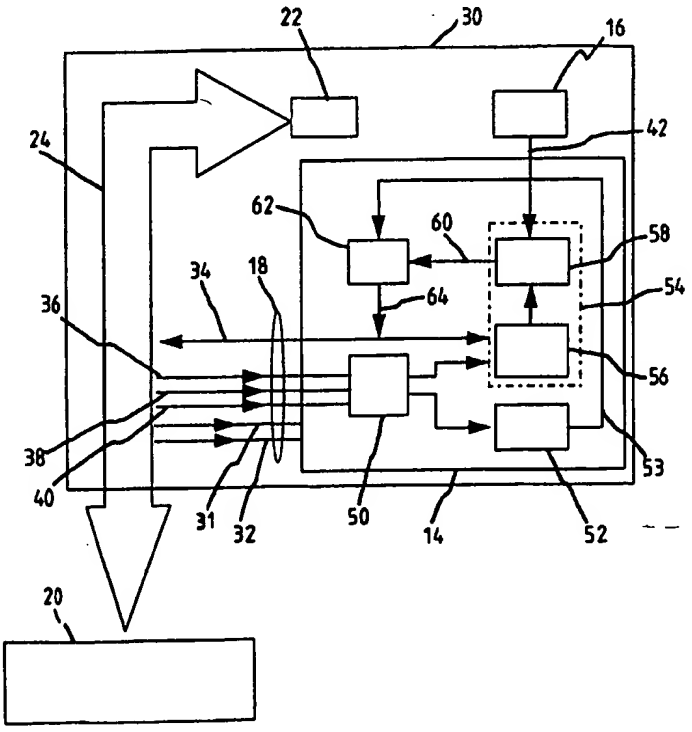
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURITY DEVICE

(57) Abstract

A computer system (10) comprises computer apparatus (12) incorporating the first and second electronic components (20, 22) and is electrically connected to a security device (14) which is associated with a non–volatile store (16) and components (12 and 14) are interconnected via a security bus (18). The security device (14) is used to protect at least one of the first electronic component (20) and the second electronic component (22) from theft and unauthorised re–use. Typically component (20) is a microprocessor for generating instructions and component (22) is a memory module for receiving instructions and outputting signals in consequence, the components (20, 22) being interconnected by a further bus (24).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Security Device

The present invention relates to a computer system. In particular, the present invention relates to a security device for preventing theft and unauthorised re-use of electronic components forming part of a computer system.

Electronic components, particularly those used in computer systems (such as memory modules, microprocessors, disk drives, and the like) are an attractive commodity to steal. This is because they are valuable, small, light, easily removed, difficult to trace once stolen, physically interchangeable, and difficult to protect from theft.

To prevent theft, the components could be securely fixed in place inside the computer system, and covered with a non-conducting material (such as a glob top). This has the disadvantage, however, that the components are no longer removable by the owner, which means that the components cannot be easily replaced, for example so as to be upgraded.

It is an object of the present invention to provide a security device for use with a computer system for preventing theft and unauthorised re-use of electronic components forming part of a computer system.

According to a first aspect of the present invention there is provided a security device for use with an electronic component forming part of a computer system, where the electronic component communicates via a plurality of signal-conveying connectors, and the security device comprises:

storage means for storing a predetermined code for use as a security code,

detection means connected to at least one of the signal-conveying connectors for detecting a signal,

comparing means responsive to the detection means for evaluating a function of the predetermined code and signals on the at least one of the signal-conveying

connectors to determine whether or not that function fulfils an acceptance criterion, and

disable means responsive to the comparing means for disabling either the electronic component or the security device.

The comparing means evaluates a function of the predetermined code and the signals detected by the detection means to determine whether or not that function fulfils an acceptance criterion. In its simplest form the function may be the subtraction of respective bits and the acceptance criterion is met if each subtraction results in a binary zero. In a more complicated form the function may be the addition of respective bits. Alternatively, the function may be another logical combination, or even a hashing function.

Preferably, the computer system simultaneously applies the same bit of the predetermined code on a plurality of the signal-conveying connectors to ensure that whichever of the signal-conveying connectors is monitored by the detection means the correct bit from the predetermined code will be detected.

Preferably, the storage means is non-volatile memory such as an EPROM or EEPROM. Alternatively, the storage means is another form of non-volatile storage such as computer hard disk, floppy diskette, CD-ROM, and the like.

Preferably, the detection means is connected to at least one control signal on the signal-conveying connectors to determine when a selected data signal is valid, and to the selected data signal on the signal-conveying connectors to monitor the value of the data signal.

Preferably, the disable means disables the electronic component by applying a fixed voltage to one of the signal-conveying connectors.

Preferably, the disable means disables the security device by disabling the output of the disable means.

Preferably, there is a delay between determining that the electronic component should be disabled and actually disabling the electronic component. Conveniently, the delay is variable. This feature has the advantage of hiding the event which caused the disable means to disable the electronic component.

In one mode of operation, the security device comprises timing means for generating a time-out signal after a period of time. The disable means is also responsive to the time-out signal for disabling the electronic device in the event that the predetermined code does not fulfil the acceptance criterion prior to generation of the time-out signal, and for disabling the security device in the event that the predetermined code does fulfil the acceptance criterion prior to generation of the time-out signal.

Preferably, the timing means counts the number of signal changes detected by the detection means until a predetermined number is reached. Alternatively, the timing means is a delay circuit comprising resistive and capacitive elements, or a shift register. Alternatively, the timing means may be a monostable circuit.

Preferably, the detection means, comparing means, timing means and disable means are implemented on an Application Specific Integrated Circuit (ASIC).

In another mode of operation, the security device comprises delay means for generating a blanking interval on initiation of power to the security device, so that operation of the security device is inhibited until after the blanking interval has elapsed. Preferably, the delay means counts the number of signal changes detected by the detection means until a predetermined number is reached. Alternatively, the delay means uses a monostable circuit, or a clock, or, the delay means waits until a predetermined state or condition is reached.

According to a second aspect of the present invention there is provided a method of disabling an electronic component having signal-conveying connectors if a predetermined code is not received, the method comprising the steps of:

storing a predetermined code for use as a security code,

detecting a signal on at least one of the signal-conveying connectors,

evaluating a function of the predetermined code and signals on the at least one of the signal-conveying connectors to determine whether or not that function fulfils an acceptance criterion, and

consequently disabling either the security device or the electronic device.

The method may further comprise the step of generating a time-out signal after a period of time if the acceptance criterion is not met.

Alternatively, or additionally, the method may further comprise the step of generating a delay on initiation of power to the security device, so that operation of the disable means is inhibited until after the delay has elapsed.

It will be understood that the host may be, for example, a computer, a motherboard, or some other component or components to which the electronic component is connected.

These and other aspects of the present invention will become apparent from the following specific embodiments, given by way of example, when taken in combination with the accompanying drawings, in which:

Fig 1 is a block diagram illustrating the electronic interconnection of computer apparatus and a security device;

Fig 2 is a block diagram of an embodiment of the

present invention where a memory module is to be protected from unauthorised use;

Fig 3 is a block diagram of an embodiment of the present invention where a microprocessor is to be protected from unauthorised use;

Fig 4 is a schematic diagram in two parts (Figs 4a and 4b) showing a specific implementation of the embodiment of Fig 2. The line A-A shows where the original schematic diagram was cut to produce Figs 4a and 4b; and

Fig 5 is an alternative embodiment of a detail of Fig 4.

Fig 1 shows part of a computer system 10 comprising computer apparatus 12, electrically connected to a security device 14, the device 14 having an associated non-volatile store 16, where the apparatus 12 and security device 14 are connected via a security bus 18. The apparatus 12 comprises a first electronic component 20 for generating instructions, which is typically a microprocessor, and a second electronic component 22 (which may be a memory module) for receiving instructions and outputting signals in response to the instructions, the first and second components 20,22 being connected by a bus 24.

The security device 14 is used to protect at least one of the first and second components 20,22 from theft and unauthorised re-use.

The non-volatile store 16 may be internal to the security device 14 or it may be external, as shown.

The bus 24 comprises a plurality of signal conveying conductors, for example insulated wire connectors or tracks disposed on a printed circuit board, typically for conveying a plurality of data signals, a plurality of address signals, a plurality of control signals, one or more power signals and one or more electrical ground signals.

The security bus 18 typically has fewer signal-

conveying conductors than the bus 24, but this is not necessarily the case, and the individual conductors in the security bus 18 are permanently connected to selected individual conductors in the bus 24.

As will be explained in more detail, one or more selected conductors on the bus 24 are used to deliver a code, issued by the first component 20, to the second component 22. The code is in the form of a sequence of n data bits applied to the selected conductor(s), where n is, for example, 64.

If the security device 14 is used to prevent unauthorised re-use of the second component 22 then at least part of the device 14 is physically connected to the second component 22 (for example, they may be mounted on a common substrate); whereas, if the device 14 is used to prevent unauthorised re-use of the first component 20 then at least part of the device 14 is physically connected to the first component 20. In either case, the security device 14 can operate in either of two modes.

In the first mode of operation, the device 14 monitors the selected conductor(s) immediately power is received by the device 14 at switch-on of the system 10. The device 14 then evaluates a function of the n bit predetermined code stored in non-volatile store 16 and bits derived from bus 24 to determine whether or not an acceptance criterion is fulfilled prior to a predetermined time interval having elapsed.

It will be understood that the predetermined time interval may be determined exactly by a clock function, or it may be determined on a variable basis in relation to the operation of the device by detecting the state of an electronic component such as a monostable, or by counting the number of occurrences of a particular event cycle on the bus 24.

It will also be understood that the security device 14

continuously monitors bits on the bus 24; however, bits are only derived from the bus 24 when a code criterion is met. The code criterion may be, for example, the logical state of one or more signals on the bus 24.

When the code criterion is fulfilled, the bits derived from bus 24 may be read directly and the logical value of the bits used as the code, or the bits read may be operated on to produce the n bit code. There are a number of ways in which the bits read may be operated on, for example, bits from the bus 24 may be operated on by a function to produce different bits, or a bit pattern may be detected to produce a single bit, or a hashing function may be applied to the bits from the bus 24.

It will also be understood that the bits from the bus 24 which are taken to form the code are not necessarily adjacent bits from the bus 24.

It will also be understood that the acceptance criterion may be fulfilled when the received code is identical to the predetermined code stored in non-volatile store 16; or it may be that acceptance criterion is some function of the predetermined code; or the acceptance criterion may be fulfilled by a predetermined condition or state being attained when the two codes are compared.

If the acceptance criterion is fulfilled then the security device 14 disables itself. If, however, the predetermined time interval has elapsed during which time the acceptance criterion is not fulfilled, then the device 14 sets one or more of the conductors in the bus 24 to a fixed voltage, thereby disabling operation of the selected component (either 20 or 22) without damaging the other component (22 or 20 respectively) or the bus 24.

In the second mode of operation, when power is applied to the device 14 at switch-on of the system 10, the device 14 waits for a blanking interval. During this blanking interval, operation of device 14 is inhibited, for example,

by arranging that the disable means is disabled. When the blanking interval has elapsed the device 14 then evaluates a function of the n bit predetermined code stored in non-volatile store 16 and bits derived from bus 24 when the code criterion is fulfilled to determine whether the acceptance criterion is fulfilled. If the acceptance criterion is fulfilled then the security device 14 disables itself. If, however, the acceptance criterion is not fulfilled then the device 14 sets one or more of the conductors in the bus 24 to a fixed voltage, thereby disabling operation of the selected component (either 20 or 22) without damaging the other component (22 or 20 respectively) or the bus 24.

Fig 2 is a block diagram of a memory module 30 which incorporates components 14, 16, 18, 22, and 24 of Fig 1, and where the security device 14 operates in the first mode (described above), with the comparing means evaluating the function of subtracting or comparing sequential bits, and the acceptance criterion being that each subtraction or comparison should produce a binary zero. The module 30 is for connection to a host computer, which is the first component 20 of Fig 1.

Memory modules are particularly vulnerable to theft because they are designed to be easily removed, they are designed to be interchangeable, and multiple modules may be used in each computer system. Memory modules are circuit boards which are populated with memory circuits to provide additional memory for a host computer, and which have a row of connectors along one side to connect to a computer motherboard. The memory circuits are equivalent to the electronic component 22 of Fig 1.

The module 30 incorporates the security device 14, the non-volatile memory 16, the security bus 18, the second component 22, and the bus 24. Generally, memory modules connect to a motherboard via a connector, so there is a bus

24 on the module 30 and also on the motherboard.

The security device 14 in Fig 2 is implemented as an ASIC with eight input/output connections (pins). One pin 31 (the connections of which are not shown internally to the security device 14) is used to receive power (Vdd), one pin 32 (the connections of which are not shown internally to the security device 14) is used to receive electrical ground (Vss), one pin 34 to receive a data bit from the bus 24, three pins 36,38,40 to receive control signals from the bus 24 (relating to the one data bit to which pin 34 is connected), one pin 42 to receive data from the non-volatile store 16, and one pin is unused.

Pin 34 is connected to data bit 9, although pin 34 could be connected to any other data bit, or any other suitable bit such as an address bit or control bit. Pin 36 is connected to the control conductor which is used to indicate when data bit 9 contains valid data, thus pin 36 is connected to RAS0. Similarly, pin 38 is connected to the column address strobe (CAS) signal for data bit 9 (CAS1). Pin 40 is connected to the write enable (WE) signal. Pins 31, 32, 34, 36, 38 and 40 comprise the security bus 18. Pins 36, 38, and 40 are active when data bit 9 contains valid data; that is, these pins (36,38,40) convey active signals when the host 20 is writing data to the memory circuits 22 on data bit 9. If a data bit other than data bit 9 was used, the pins 36,38,40 would be connected to the appropriate signals which define a write cycle for the data bit chosen. This information (the signals which, when active, define which particular data bits contain valid data) is available from standard data books (published by memory module suppliers) and text books relating to memory modules. The non volatile store 16 is a one-time programmable ROM which is programmed with a predetermined 64 bit code. In other embodiments the predetermined code may be longer or shorter than 64 bits.

The predetermined code is entered into a computer program for installing in the computer 20 connected to the module 30.

In use, the module 30 and computer program containing the predetermined 64 bit code are installed in the computer system 10; thereafter, the computer system 10 is switched on. When the computer 20 receives power, the microprocessor within the computer 20 executes an initialisation procedure, during which the computer 20 determines, amongst other things, how much memory is present. During at least part of the initialisation procedure the memory module 30 will be accessed by the computer 20 and the computer 20 may write data to the module 30.

When power is first applied to the security device 14, timing means 52 is used to ensure that the security device 14 will disable the module 30 if the correct code is not received within a predetermined time limit (in accordance with the first mode of operation of device 14 previously explained). This has the advantage that there is only a limited amount of time in which unauthorised users can attempt to generate the correct code. The timing means 52 is connected to detection means 50 for counting the number of refresh cycles using pins 36 and 38, and generates a time-out signal 53 once a predetermined count value is reached.

Once the computer 20 has finished at least part of the initialisation procedure (which may take several minutes for some systems) then the program storing the predetermined code is executed. This program is accessed by the computer 20 from a store within the computer 20 during the initialisation procedure, and causes the computer 20 to write the predetermined code to the memory module 30 via bus 24. The computer 20 simultaneously writes the same bit of the 64 bit code on each data

conductor in the bus 24 to ensure that whichever conductor on the bus 24 is monitored by the device 14, at any given moment in time, the correct bit from the predetermined code will be seen. Thus, the first bit of the code is written on each data conductor, then the second bit of the code is written on each data conductor, and so on until all 64 bits of the code have been written on all of the data conductors, so that whichever data conductor is monitored the correct sequence of 64 bits will be detected. This obviates any problems which may arise due to the computer 20 scrambling the data prior to outputting the data to the data conductors on the bus 24.

The computer program in this embodiment ensures that the predetermined code is applied as an unbroken sequence, for example, by ensuring that the code is not broken by interrupt servicing. However, in other embodiments, the code may be interrupted by design, in which case the security device is arranged to filter the received signals to restore the unbroken code.

If more than one module 30 is used in a computer system 10 then there is a corresponding number of security devices 14, each with a different code. The predetermined codes (one for each security device) are written in sequence by the computer 20, thus the first predetermined code is written, then the next predetermined code is written, and so on until all of the predetermined codes have been written. If a particular security device 14 receives a block of 64 bits which does not match the predetermined code, then the device 14 ignores that block and waits to receive another block of 64 bits for comparing with the predetermined code. Thus, the various security devices 14 may receive any number of incorrect codes before each device 14 receives the correct code, provided the correct code is received prior to the respective timing means 52 generating the time-out signal 53.

When the computer 20 writes the predetermined code to the module 30, the detection means 50 detects that a write operation has been initiated because of the state of the electrical signals on pins 36, 38 and 40. The output of detection means 50 then responds by controlling comparing means 54, which comprises a 64 bit shift register 56 and a comparator 58, so that the shift register 56 receives and stores data from pin 34. The comparator 58 independently receives and stores bits from the non-volatile store 16 which are sent serially via pin 42. The comparator 58 then compares in parallel the bits from the non-volatile store 16 with the bits from the shift register 56 on a bit by bit basis and, at the end of each 64 bit sequence, outputs a single comparison bit 60. The single comparison bit 60 is input to disable means 62. The time-out signal 53 is also connected to the disable means 62.

If the time-out signal 53 goes active (indicating that the predetermined count has been reached) prior to the comparison bit 60 going active, then the disable means 62 sets its output 64 to Vdd, ensuring that there will be a memory failure when the computer 20 attempts to write a logic zero onto data bit 9.

If the single comparison bit 60 goes active (indicating that there is a match between the predetermined code and the code written by the computer program) prior to the time-out signal 53 going active, then the disable means 62 is disabled so that data bit 9 is not affected by the security device 14.

When power is removed from the computer system the security device 14 is reset so that when power is reapplied the device 14 must again receive the correct code before the device 14 will be disabled.

If the security device 14 is connected to a circuit board then the device 14 should be mounted in such a way as to make removal or bypassing of the device extremely

difficult. For example, the device 14 and connections (particularly pin 34) may be covered with a material which is difficult to remove, for example a glob top, or the connections to the security device may be made by tracks routed through the centre of the circuit board.

Table 1 gives an example of a computer program for use with the above embodiment, which may be used to write a predetermined code to the device 22.

Fig 3 is a block diagram of an embodiment of the present invention where a microprocessor is to be protected from unauthorised use. The first component 20 is a microprocessor, the second component 22 may be a memory module, motherboard, or the like. The microprocessor 20, the security device 14, the non-volatile store 16, and the security bus 18 are incorporated into a custom microprocessor 66. Within the custom microprocessor 66, there are similar components to the components described for the Fig 2 embodiment, like numerals relate to like components. The main difference between the embodiments of Figs 2 and 3 is that pins 36, 38 and 40 (which connect to WE, RAS, and CAS control signals in the Fig 2 embodiment) connect to different control signals (WE) in the Fig 3 embodiment.

Fig 4 shows a specific implementation of the embodiment of Fig 2. There is a 68 bit shift register 70 for receiving and storing the predetermined code from the non-volatile store (not shown) via pin 42. 64 bits of the output 72 (which comprises the predetermined code output 73) of the shift register 70 are connected to the comparator 58. The remaining four bits are connected elsewhere in the circuit, as will be described below.

The comparator 58 is an array of 64 exclusive NOR logic gates 74 (only one is shown for clarity) with additional logic at the 64 outputs of the XNOR gates 74 to generate a single output 75 from the 64 outputs. The other

input to the comparator 58 is from the output of the 64 bit shift register 56. The shift register 56 receives data from data line 9 via pin 34.

The detection means 50 comprises logic gates to detect the state of pins 36, 38 and 40 which exists when a write cycle is being initiated. The timing means 52 comprises logic circuitry to detect when a refresh cycle is being initiated and to count refresh cycles (using a 30 stage counter). There is also a multiplexor 80 to provide a degree of programmability in the length of time which elapses before the time-out signal 53 is generated.

The multiplexor has three inputs 82 from the 68 bit shift register 70. Thus, the non-volatile store 16 can be programmed with an additional three bits to determine the delay before the time-out signal 53 is generated. This provides flexibility and is useful when the security device is used with computer systems which take longer than usual to initialise (for example, several minutes).

The time-out signal 53 is connected to the disable means 62. The disable means 62 has an AND gate 90 with an input from the final bit of the 68 bit shift register 70 and an input from an initialisation line 92. The final bit of the 68 bit shift register is used as a disable bit so that the operation of the security device can be permanently disabled by setting the final bit of the shift register 70 to logic zero. The output of the AND gate 90 is used to reset a register 94 which produces output 64. Output 64 is used to drive data bit 9 to a permanent high voltage, thus ensuring incorrect operation of the module.

The security device 14 of the present invention could also be used to protect other types of electronic components. For example, the security device 14 could be used to protect a microprocessor, in which case, the security device 14 may be connected to one or more control lines on the microprocessor and a data line on the

microprocessor. The operation of the device would be very similar to that described for Figs 1 to 3. However, the microprocessor would perform the function of both the host 20 and the electronic device 22. This is because microprocessors generate, amongst other things, the addresses and control signals in computer systems. Thus, the microprocessor would be used to generate the predetermined code (from a computer program), and the security device would monitor the appropriate pins (for example, a data pin and the write enable pin) of the microprocessor to determine when the code was being issued by the microprocessor. If the correct code was not detected prior to the time-out signal going active then the security device would drive one of the microprocessor pins to Vdd. This would disable operation of the microprocessor. Alternatively, the security device may be incorporated into the micro-instruction sequencer of a microprocessor; the security device could then disable the microprocessor by changing data in the data path.

Fig 5 shows an alternative circuit for detecting refresh cycles. The circuit of Fig 5 is identical to the timing means 52 of Figs 4a and 4b except for the additional circuitry 100 which is used to exclude the possibility of detecting a certain type of cycle which is not a refresh cycle but which may be detected if the additional circuitry 100 was not present.

In other embodiments of the present invention, the security device 14 operates in the second mode, previously described with reference to Fig 1. In the second mode of operation, delay means is used to ensure that the computer 20 has completed the initialisation procedure before the security device 14 begins to check for the correct code. Thus, no code is received or stored prior to completion of the initialisation procedure. This is necessary if the security device 14 disables itself once an incorrect code

is received (unlike the Fig 2 and Fig 4 embodiments where the security device may receive any number of incorrect codes) provided the correct code is received prior to the time-out signal being generated. The delay means is necessary to ensure that any incorrect code which is inadvertently issued by the host 20 during the initialisation procedure is ignored by the security device 14. The host 20 may inadvertently issue a code by, for example, writing data to a memory location.

The delay means may be determined by use of a clock located within or outside the security device 14. Alternatively, the delay means may be incorporated into the detection means 50 so that when power is first applied to the security device 14, the detection means 50 counts a predetermined number of, for example, refresh cycles. This would provide a delay to ensure that the computer 20 has finished the initialisation procedure before the correct code is sent to the electronic component 22. The number of refresh cycles which are counted (the length of the delay) may be a programmable option.

In other embodiments different means may be used to implement the disable function. For example by electronically disrupting a signal path or by driving a signal (such as data bit 9 in the Figs 2 and 4 embodiments) to a fixed voltage such as electrical ground voltage, or by using logic circuitry to invert a signal or disable a buffer. In embodiments which use a security device to protect a microprocessor the disable means may be used to garble the data generated by the microprocessor.

Pin 34 may be connected to any convenient conductor, for example any data conductor; or to any other convenient conductor, for example a conductor conveying an address signal or a control signal. If pin 34 was connected to an address signal then the host 20 would issue an address which would be considered as the code. For example, the

security device 14 would monitor an address bit and if the sequence of signals on the address bit did not match the predetermined code then the address bit would be set to Vdd.

In other embodiments, the security device 14 may be incorporated into the electronic device 22 which it is protecting. Where the electronic device 22 is fabricated as an integrated circuit then the security device 14 may be designed as part of the integrated circuit. Where a memory module controller is used for controlling memory redundancy, the security device 14 may be incorporated into the memory module controller; alternatively, the security device may be incorporated into a standard microprocessor.

The eight pin package described in the Fig 2 embodiment is given merely by way of example, other sizes and types of packaging (including no packaging) are possible.

In other embodiments the predetermined code may be embedded into the security device 14 during manufacture to obviate the need for an external non-volatile store 16.

The predetermined code in the above embodiments is a single 64 bit code which is applied to a single data line. However, in other embodiments, a plurality of codes may be applied to a plurality of data lines simultaneously. For example, a first 64 bit code may be applied to one conductor (data bit 9) and a second 64 bit code may be applied simultaneously to a second conductor (data bit 8). Both conductors would be monitored simultaneously and the codes which are received on the two conductors compared with two predetermined codes which are stored in the non-volatile store. The codes which are stored in the non-volatile store may be retrieved as serial data via a single conductor, or there may be two conductors to retrieve the data in parallel. Only if each of the received codes matches the corresponding code from the non-volatile store

is the security device disabled. This is a more complex embodiment because, for example, all of the data lines cannot convey the same data at any given time. If there is any scrambling of the data lines then the scrambling algorithm must be known so that the correct data is applied to the correct data line, or the timing sequence of the code requires to be reconstructed using inverse hashing.

In other embodiments, the computer program which writes the predetermined code to memory may prompt the user to enter the code manually to avoid it being held in a local store which might be accessible to an unauthorised user who might thereby retrieve the code.

```
JUMPS

.model  small
.stack  100h

.code
.486p

start:  JMP     strt

mess:   db      "this is an internal test message",13,10,"$"
cr:     db      13,10,"$"
rlword: db      "01234567 $"
rword:  db      "0123 $"
rbyte:  db      "01 $"

pat1:   dd      00000000h
pat2:   dd      0ffffffffh
pat3:   dd      00000000h
pat4:   dd      00000000h
pat5:   dd      0ffffffffh
pat6:   dd      0ffffffffh
pat7:   dd      00000000h
pat8:   dd      00000000h
pat9:   dd      00000000h
pat10:  dd      0ffffffffh
pat11:  dd      0ffffffffh
pat12:  dd      0ffffffffh
pat13:  dd      00000000h
pat14:  dd      00000000h
pat15:  dd      00000000h
pat16:  dd      00000000h
pat17:  dd      0ffffffffh
pat18:  dd      0ffffffffh
pat19:  dd      0ffffffffh
pat20:  dd      0ffffffffh
pat21:  dd      00000000h
pat22:  dd      00000000h
pat23:  dd      00000000h
pat24:  dd      00000000h
pat25:  dd      00000000h
pat26:  dd      0ffffffffh
pat27:  dd      0ffffffffh
pat28:  dd      0ffffffffh
pat29:  dd      0ffffffffh
pat30:  dd      0ffffffffh
pat31:  dd      00000000h
pat32:  dd      00000000h
pat33:  dd      00000000h
pat34:  dd      00000000h
pat35:  dd      00000000h
pat36:  dd      00000000h
pat37:  dd      0ffffffffh
pat38:  dd      0ffffffffh
pat39:  dd      0ffffffffh
pat40:  dd      0ffffffffh
pat41:  dd      0ffffffffh
pat42:  dd      0ffffffffh
pat43:  dd      00000000h
pat44:  dd      00000000h
pat45:  dd      00000000h
pat46:  dd      00000000h
pat47:  dd      00000000h
```

Table 1

```
pat48:  dd      00000000h
pat49:  dd      00000000h
pat50:  dd      0ffffffffh
pat51:  dd      0ffffffffh
pat52:  dd      0ffffffffh
pat53:  dd      0ffffffffh
pat54:  dd      0ffffffffh
pat55:  dd      0ffffffffh
pat56:  dd      0ffffffffh
pat57:  dd      00000000h
pat58:  dd      00000000h
pat59:  dd      00000000h
pat60:  dd      00000000h
pat61:  dd      00000000h
pat62:  dd      00000000h
pat63:  dd      00000000h
pat64:  dd      00000000h
pat65:  dd      0ffffffffh
pat66:  dd      0ffffffffh
pat67:  dd      0ffffffffh
pat68:  dd      0ffffffffh
pat69:  dd      0ffffffffh
pat70:  dd      0ffffffffh
pat71:  dd      0ffffffffh
pat72:  dd      0ffffffffh

prcr:   mov     dx,offset cr                    ;output CR and LF
        mov     ah,9
        int     21h
        ret

prlword:mov     di,offset rlword                ;output 32-bit word
        rol     eax,8
        call    hex
        rol     eax,8
        call    hex
        rol     eax,8
        call    hex
        rol     eax,8
        call    hex
        mov     dx,offset rlword
        mov     ah,9
        int     21h
        ret

prword: mov     di,offset rword                 ;output 16-bit word
        rol     ax,8
        call    hex
        rol     ax,8
        call    hex
        mov     dx,offset rword
        mov     ah,9
        int     21h
        ret

prbyte: mov     di,offset rbyte                 ;output 8-bit byte
        call    hex
        mov     dx,offset rbyte
        mov     ah,9
        int     21h
        ret

hex:    push    ax                              ;byte0 - hex to ascii
        and     ax,0fh
```

Table 1 (continued)

```
        cmp     ax,0ah
        jl      hex1
        sub     ax,0ah
        add     ax,"A"
        jmp     hex2
hex1:   add     ax,"0"
hex2:   mov     dx,ax
        rol     dx,8
        pop     ax
        push    ax
        ror     ax,4
        and     ax,0fh
        cmp     ax,0ah
        jl      hex3
        sub     ax,0ah
        add     ax,"A"
        jmp     hex4
hex3:   add     ax,"0"
hex4:   add     ax,dx
        mov     [di],ax
        add     di,2
        pop     ax
        ret

strt:   push    ds                              ;save ds
        push    cs                              ;make ds same as cs
        pop     ds


        mov     eax,cr0                         ;output cr0
        call    prlword

        mov     eax,cr0                         ;read control
register
        or      eax,60000000h                   ;set cache control
bits
        mov     cr0,eax                         ;disable cache

        mov     eax,cr0                         ;check values
        call    prlword

        wbinvd                                  ;flush cache

        mov     eax,cr0                         ;check values
        call    prlword
        call    prcr

        mov     bx,50000

lp2:    mov     cx,72
        mov     si,offset pat1

        cli                                     ;disable interrupts

        mov     di,offset rbyte                 ;output 8-bit byte
        mov     [di],0aaaaaaaah                 ;output marker

        mov     di,offset rlword


lp1 :   mov     eax,[si]
        mov     [di],eax
```

Table 1 (continued)

```
add     si,4
dec     cx
jnz     lp1

sti                                     ;enable interrupts


dec     bx
cmp     bx,0
jne     lp2


wbinvd

mov     eax,cr0                         ;check values
call    prlword
call    prcr

pop     ds

mov     ah, 4ch     ; Return to DOS
int     21h

end
```

Table 1 (continued)

CLAIMS

1. A security device for use with an electronic component forming part of a computer system, where the electronic component communicates via a plurality of signal-conveying connectors, and the security device comprises:

storage means for storing a predetermined code for use as a security code,

detection means connected to at least one of the signal-conveying connectors for detecting a signal,

comparing means responsive to the detection means for evaluating a function of the predetermined code and signals on the at least one of the signal-conveying connectors to determine whether or not that function fulfils an acceptance criterion, and

disable means responsive to the comparing means for disabling either the electronic component or the security device.

2. A security device as claimed in claim 1 wherein the comparing means evaluates a function of the predetermined code and the signals detected by the detection means to determine whether or not that function fulfils an acceptance criterion, the function being the subtraction of respective bits, and the acceptance criterion is met if each subtraction results in a binary zero.

3. A security device as claimed in either preceding claim wherein the computer system simultaneously applies the same bit of the predetermined code on a plurality of the signal-conveying connectors to ensure that whichever of the signal-conveying connectors is monitored by the detection means the correct bit from the predetermined code

will be detected.

4. A security device as claimed in either preceding claim wherein the detection means is connected to at least one control signal on the signal-conveying connectors to determine when a selected data signal is valid, and to the selected data signal on the signal-conveying connectors to monitor the value of the data signal.

5. A security device as claimed in either preceding claim wherein the disable means disables the electronic component after a delay between determining that the electronic component should be disabled and actually disabling the electronic component.

6. A security device as claimed in either preceding claim wherein the security device comprises timing means for generating a time-out signal after a period of time and the disable means is also responsive to the time-out signal for disabling the electronic device in the event that the predetermined code does not fulfil the acceptance criterion prior to generation of the time-out signal, and for disabling the security device in the event that the predetermined code does fulfil the acceptance criterion prior to generation of the time-out signal.

7. A security device as claimed in any one of claims 1 - 5, wherein the security device comprises delay means for generating a blanking interval on initiation of power to the security device, so that operation of the security device is inhibited until after the blanking interval has elapsed.

8. A method of disabling an electronic component having signal-conveying connectors if a predetermined code

is not received, the method comprising the steps of:

storing a predetermined code for use as a security code,

detecting a signal on at least one of the signal-conveying connectors,

evaluating a function of the predetermined code and signals on the at least one of the signal-conveying connectors to determine whether or not that function fulfils an acceptance criterion, and

consequently disabling either the security device or the electronic device.

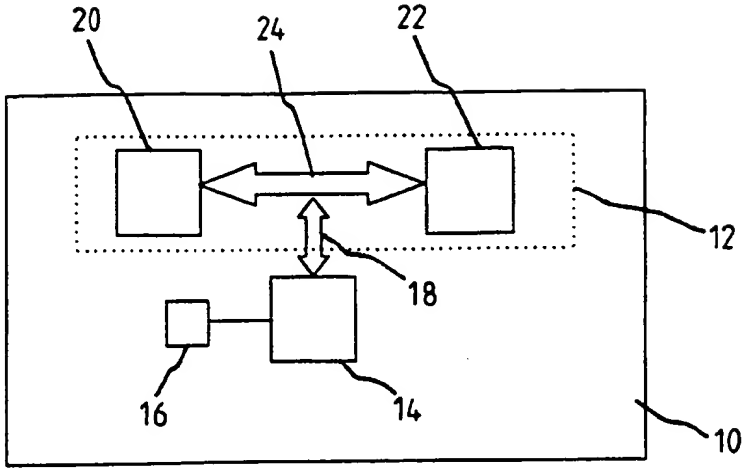


FIG. 1

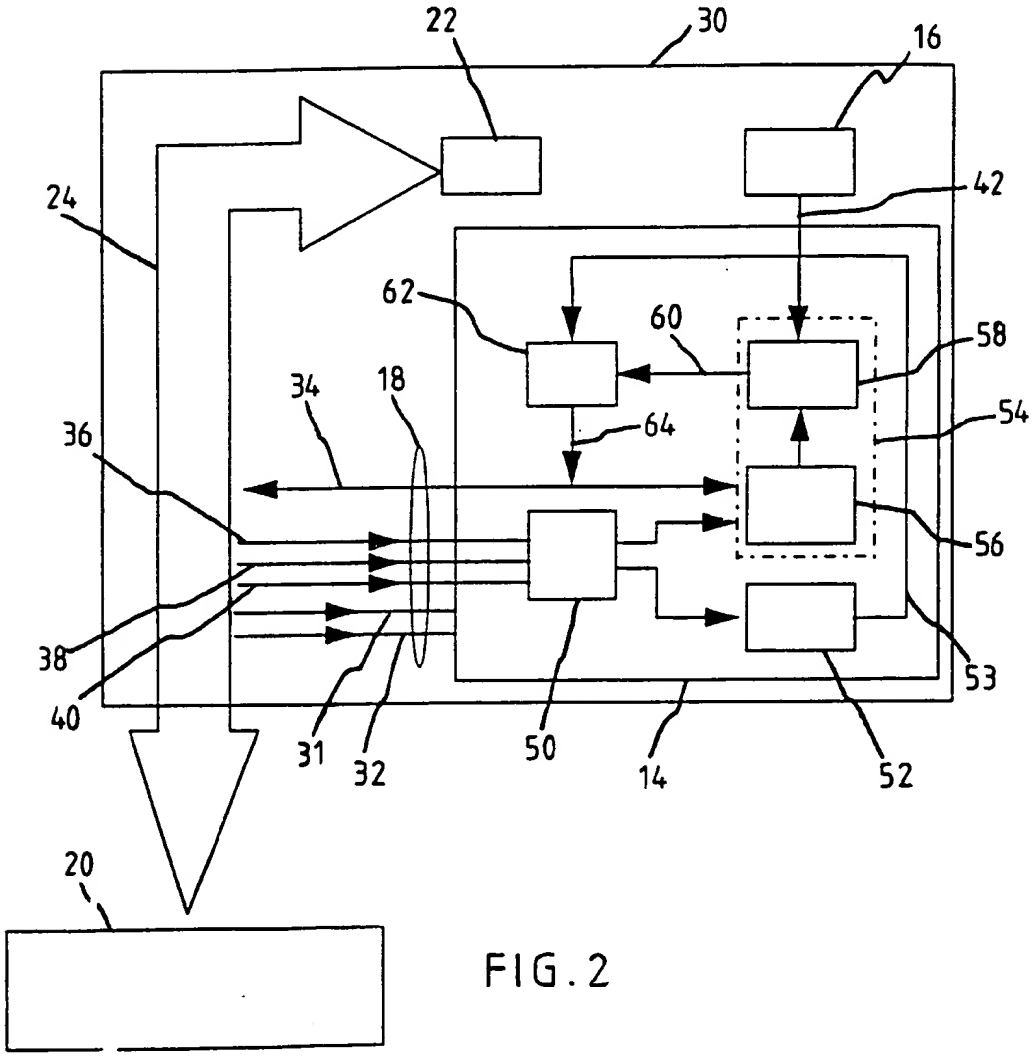


FIG. 2

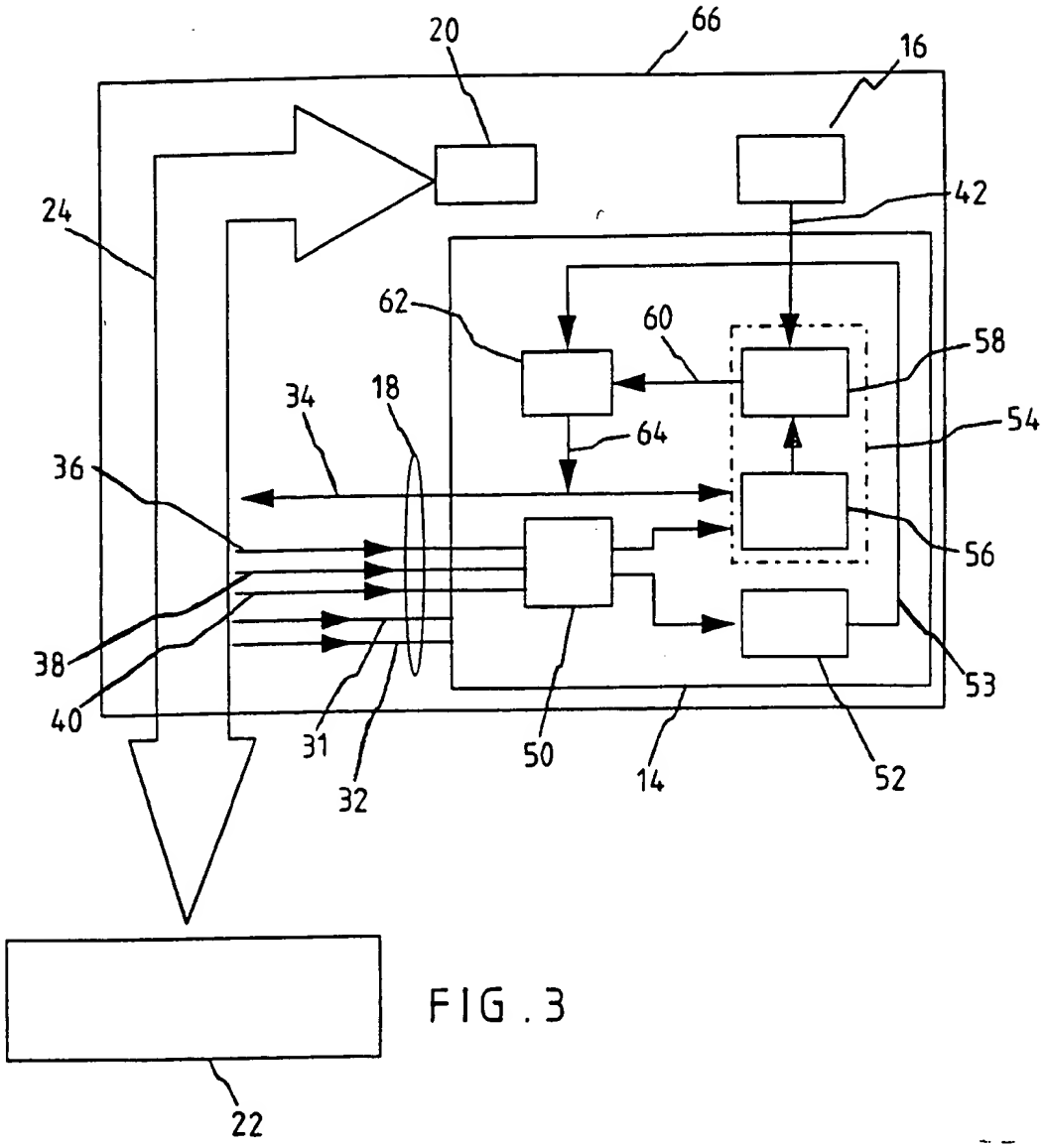


FIG. 3

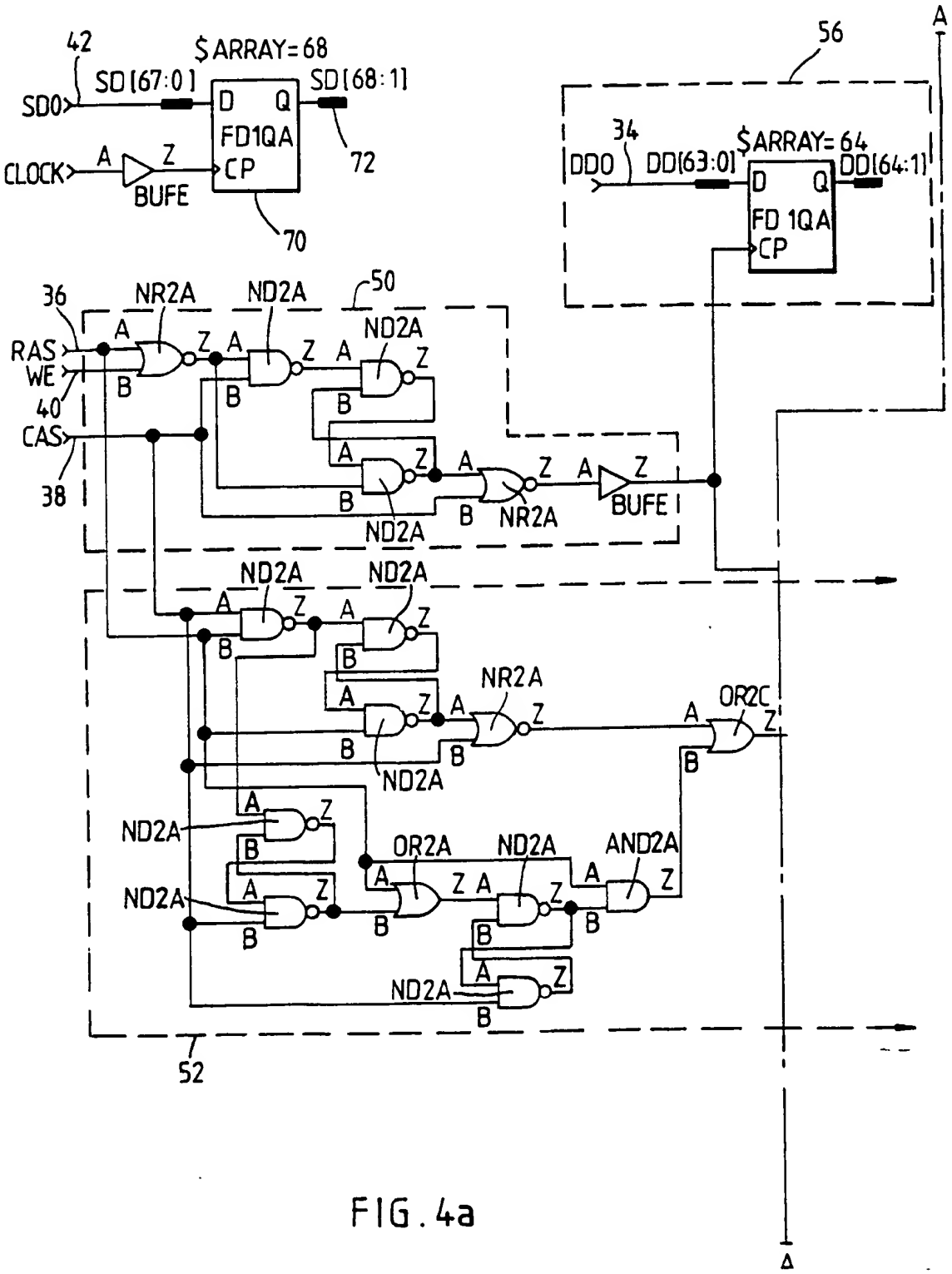


FIG. 4a

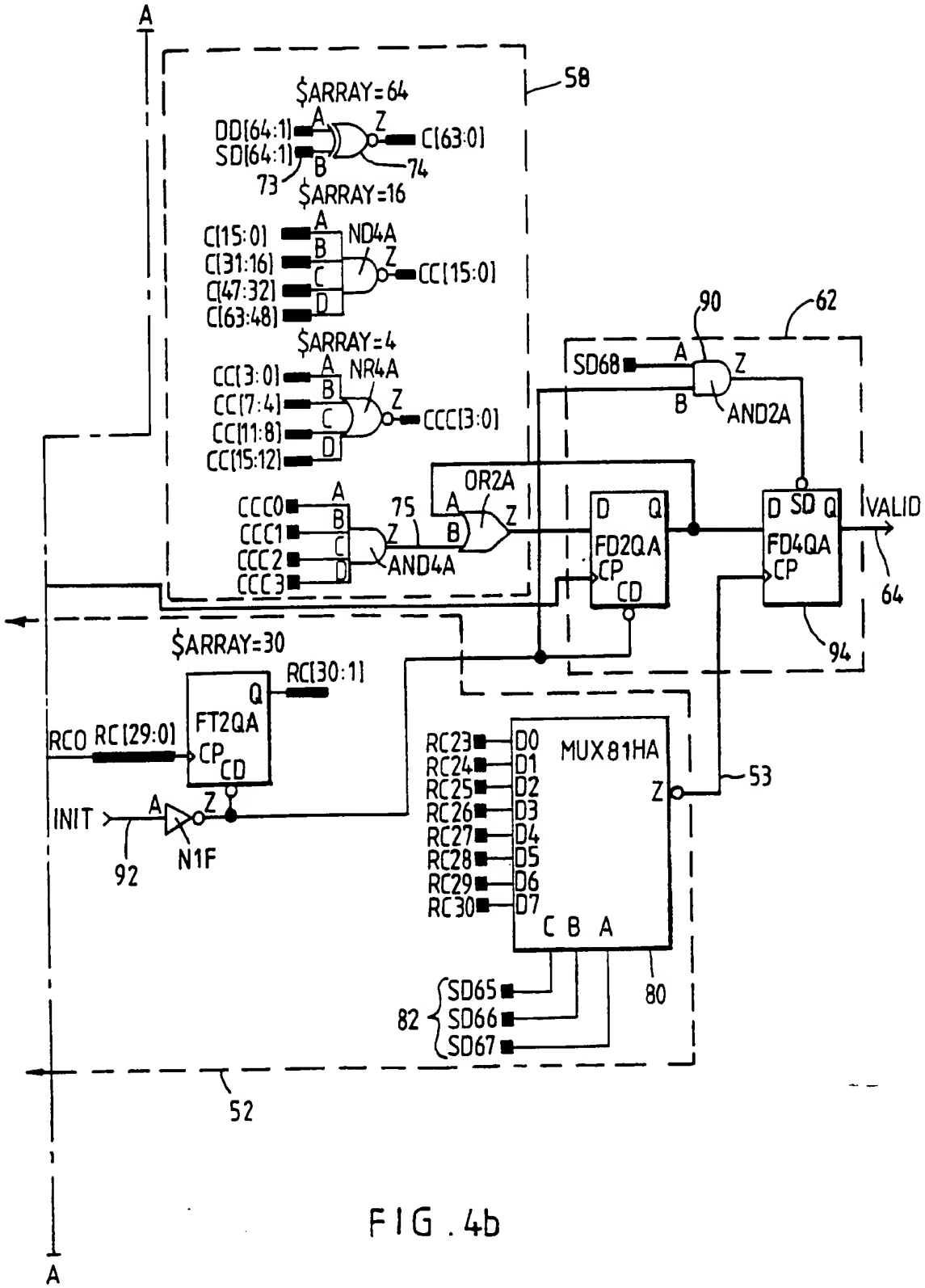


FIG. 4b

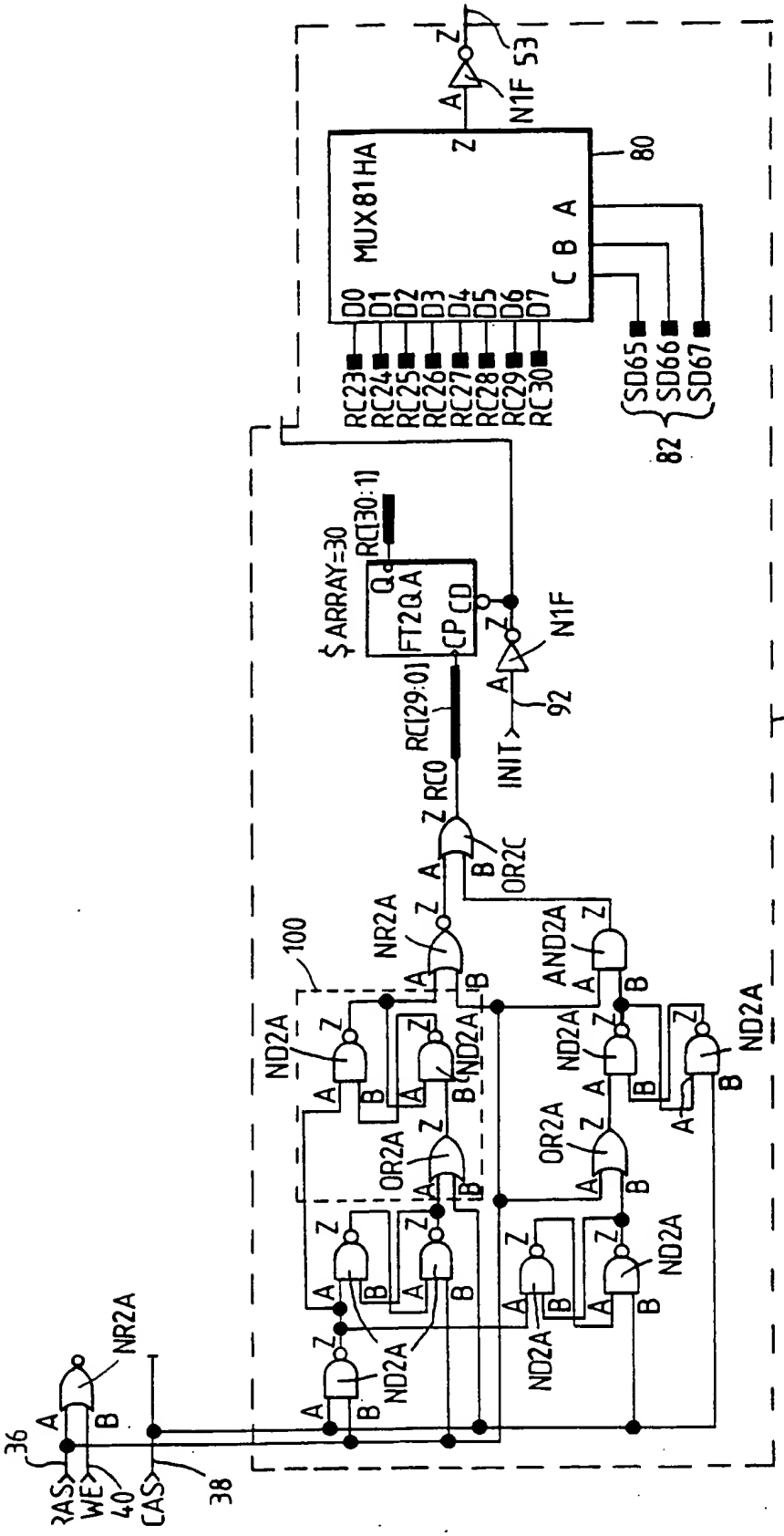


FIG. 5

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 98/01705

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 864 542 A (OSHIMA TOSHIO ET AL) 5 September 1989 see column 2, line 45 - column 3, line 16; figure 1 see column 3, line 44 - column 5, line 43 ---	1,8
Y	EP 0 175 359 A (WANG LABORATORIES) 26 March 1986 see page 7, line 1 - line 20; claim 1; figure 1 ---	1,8
Y	DE 295 19 865 U (SIEMENS AG) 23 January 1997 see page 1, line 18 - line 24; claim 1; figure 1 see page 2, line 19 - line 27 --- -/--	1,8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 October 1998	12/10/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Breusing, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. ınal Application No
PCT/GB 98/01705

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A,P	EP 0 798 620 A (LUCENT TECHNOLOGIES INC) 1 October 1997 see page 3, line 10 - line 31; figure 1 ---	1
A	DE 41 20 864 A (MITAC GMBH) 10 September 1992 see abstract; figure 3 ---	1
A	EP 0 425 053 A (TRT TELECOM RADIO ELECTR ;PHILIPS NV (NL)) 2 May 1991 see column 6, line 39 - column 7, line 38; figure 1 ---	1,2,8
A,P	WO 97 45780 A (TOERNGREN BENGT ;ALINGSAAS INFORMATION SYSTEM A (SE); JOHANSSON CH) 4 December 1997 see page 2, line 14 - page 3, line 30; figures 1,3 ---	1,8
A,P	PATENT ABSTRACTS OF JAPAN vol. 098, no. 006, 30 April 1998 & JP 10 049493 A (NEC NIIGATA LTD), 20 February 1998 see abstract -----	1

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 98/01705

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4864542 A	05-09-1989	JP 63225841 A	20-09-1988
EP 0175359 A	26-03-1986	AU 581011 B	09-02-1989
		AU 4564685 A	27-03-1986
		CA 1231457 A	12-01-1988
		DE 3585350 A	19-03-1992
		JP 61077951 A	21-04-1986
DE 29519865 U	23-01-1997	EP 0779569 A	18-06-1997
EP 0798620 A	01-10-1997	US 5774545 A	30-06-1998
		CA 2196482 A	29-09-1997
		JP 10083354 A	31-03-1998
DE 4120864 A	10-09-1992	NONE	
EP 0425053 A	02-05-1991	FR 2653914 A	03-05-1991
		JP 3152653 A	28-06-1991
		US 5146499 A	08-09-1992
WO 9745780 A	04-12-1997	AU 3111897 A	05-01-1998